مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Insyde BIOS SMM Affects HP Systems

Tracking #:432318663

Date:26-03-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in HP PC products utilizing InsydeH20 UEFI firmware. The flaw exists within System Management Mode (SMM) and may allow a privileged attacker to execute arbitrary code at the firmware level.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE ID:** CVE-2025-10451
- **Severity:** High **CVSS Score:** 8.2 (CVSS v3.1)
- The vulnerability is caused by improper memory handling within System Management Mode (SMM) in InsydeH20 UEFI firmware. SMM operates at a highly privileged level below the operating system, making it a critical attack surface.
- An attacker with elevated privileges could exploit this flaw to execute arbitrary code in SMM, potentially leading to:
  - Full system compromise
  - Firmware-level persistence
  - Bypass of OS-level security controls

Affected Products

- HP 15-dw1xxx / 15s-du1xxx / 15s-dr1xxx / 15s-dy1xxx / 15t-dw100
- HP 14-cf2xxx / 14s-cf2xxx / 14s-cr2xxx / 14s-cs2xxx / 14-ma2xxx
- HP 14t-cf200 / 14t-ma200
- HP 240 G7 / 246 G7 / 250 G7 / 255 G7 / 256 G7 / 258 G7
- HP 340 G7 / 348 G7

Note:
Refer to the official HP advisory for the full list of affected products, Fixed versions and additional information.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by HP.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://support.hp.com/us-en/document/ish_14547790-14547813-16/hpsbhf04103